least one alternative cryptographic algorithm and providing its associated public key; and

providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

cl 3 cont

5. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 3, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

6. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 3, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

## REMARKS

In the Office Action, the Examiner noted that Claims 1 through 3 were pending in the Application. The Examiner rejected all claims. In this Amendment, Applicant has added new Claims 4 - 6. Applicant traverses the rejections below.

I. Traversal of the Rejection over the Cited Art

The Examiner rejected Claims 1 through 3 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al. Applicant traverses this rejection below.

Applicant notes that Shear apparently has not been made of record in a Form PTO-892 or